

HOLODECK

BY SECURITY INNOVATION

It Wrecks Your Software ... *so your customers can't!*

Software testing is all about finding defects in applications, but it's never an easy job. It's nearly impossible to test software under all of the conditions it will run in, and even more difficult to understand how an application will react if the execution environment suddenly becomes hostile. For example, what happens if the hard disk or a network card fails or the application's configuration files are corrupted? What happens if memory is no longer available? Does the application become unstable or leave any type of data for hackers to exploit if it crashes? These events happen all the time in the real world, so why are they so often missed in testing? Because those situations are very difficult to create
...but not with Holodeck

Holodeck is a powerful fault-injection tool

that allows Microsoft® Windows™ testers to effectively simulate hostile environments to run in. Exposing applications to runtime faults forces applications to react in ways testers would not normally see. This allows testers to provide the critical feedback developers must have to generate the defensive code needed to manage applications in the *real* world where the runtime environment cannot be tightly controlled. By destabilizing the application in the lab, it can be more stable and secure in a broader array of environments outside of it.

Some hostile environmental simulations Holodeck provides are:

Resource Starvation

- Limit Memory, Disk Space and Network Bandwidth

System Faults

- Inject disk faults such as File Locked, File In Use or Data Error
- Inject network faults such as No Ports or Network Down
- Inject memory faults such as Segment Locked or Invalid Access
- Inject registry faults such as Value Not Found or Key is Corrupt
- Inject process faults such as Process Not Found or Invalid File

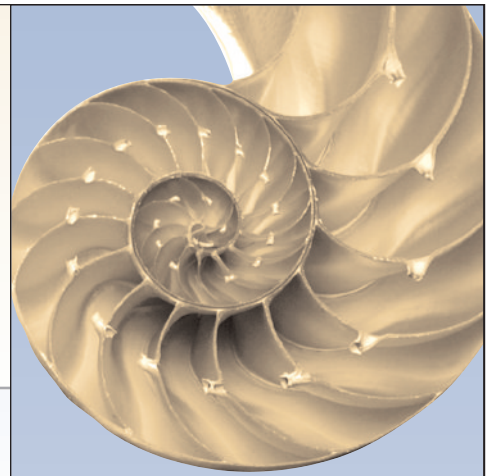
Dependency Corruption

- Generate corrupt resource files and network data streams
- Generate unexpected API return values and data
- Make COM objects disappear

Add Holodeck to your development process and join the growing global software community focused on delivering more stable and more secure applications.



Download Holodeck today:
www.securityinnovation.com/holodeck



Read about Holodeck in:

- [The Software Vulnerability Guide Thompson & Chase](#)
- [How to Break Software Security Whittaker & Thompson](#)
- [How to Break Software Whittaker](#)
- Dr. Dobbs Journal
- SQE Magazine

Use it to:

- Crash applications to expose software failures missed by exception handlers
- Expose sensitive data that hackers can exploit
- Force execution of error recovery-routines that applications may have to use in adverse conditions

Combine with key developer and test tools:

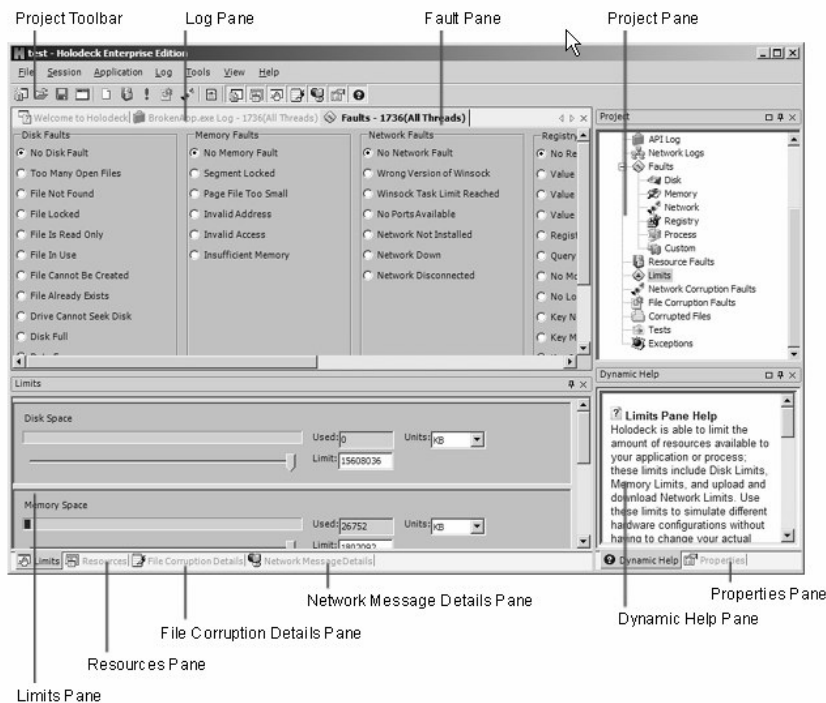
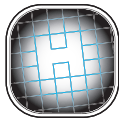
- Use with automated test tools to stress applications and force crashes
- Use with code coverage tools to drive error paths during automated and manual test runs
- Use with debuggers to locate problem code in real time

Used by many well known software vendors including **Adobe, McAfee, Microsoft and Symantec**

Proud Partners of **IBM, Microsoft and Compuware**

MORE ABOUT HOLODECK ►

HOLODECK GUIDED TOUR



The UI. Holodeck provides an easy to use interface that enables testers and developers to rapidly leverage all the power the system provides. Each step in the test setup and execution process is well documented and navigates the user effectively, regardless of task complexity.

- Project toolbar** – Contains items pertaining to your current and future projects
- Log Pane** – Displays all the APIs Holodeck is currently intercepting
- Faults Pane** – Used to set faults that confound the application under test
- Project Pane** – Manages display and organization of project tree view
- Limits Pane** – Allows limiting of available disk, memory and networking resources
- Resource Pane** – Displays the file, folder, process, library and registry resources in use
- File Corruption Details Pane** – Provides quick access to file corruption details
- Network Message Details Pane** – Displays byte data transferred with each network message
- Dynamic Help Pane** – Provides a guide through key system usage scenarios
- Properties Pane** – Provides additional information about the current UI

How it works. Holodeck uses Security Innovation's proprietary API intercept technology to get between the application and the Windows operation system and/or .Net runtime environment. It intercepts calls to the O/S and provides return values based on the configuration the user specifies. Because the application under test is never aware that it is not talking directly to the O/S, Holodeck is free to provide the application with return values that simulate the faults the user specifies. Simple, and dramatically effective!

KEY BENEFITS

For Testers

- Speeds testing process by forcing error conditions of all types
- Helps testers expose defects deeper in the application
- Helps improve application security by forcing conditions that expose key application data that a hacker may exploit
- Enhances existing test automation by forcing broader code coverage during script execution
- Helps improve application performance by exposing system bottlenecks
- Improves code coverage by forcing applications down difficult to exercise error paths
- Improves tester and development communication by creating reproducible failure scenarios

For Developers

- Speeds debugging by allowing debugger attachment to get to the root of the problem quickly
- Enhances understanding by profiling all API calls and displaying parameter data and return values



SECURITY INNOVATION®

U.S. Headquarters

187 Ballardvale Street, Suite A170
Wilmington, MA 01887 USA
Ph.: +1.978.694.1008
Fax: +1.978.694.1666

European Headquarters

ITO Building, 13th floor
Gustav Mahlerplein 54
1082 MA Amsterdam, The Netherlands
Ph: +31 (0) 20 301 9150
Fax: +31 (0) 20 301 9159

U.S. Technical Lab - West

701 Fifth Avenue, Suite 4200
Seattle, WA 98104 USA